Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs	)	WC Docket No. 18-89
	)	
	)	

COMMENTS OF MOTOROLA SOLUTIONS, INC.

Motorola Solutions, Inc. ("MSI") respectfully submits these comments in the above-captioned proceeding.[1] MSI supports the efforts of the Federal Communications Commission ("FCC" or "Commission") to promote the security and integrity of the nation's communications networks. As the Commission stated, threats posed by certain communications equipment providers have long been a matter of concern to the executive branch and to Congress,[2] and we fully agree that the Commission must play an active role to promote and safeguard the security of the Nation's telecommunications networks from such threats – consistent with the Commission's core statutory mandate to protect the reliability and resiliency of these networks.

As most recently observed by Chairman Pai's office "[M]ore than 80 years ago, our Congress had the foresight to understand that the reliability and resiliency of our communications networks was a public safety and national security issue."[3] Consistent with that

---

1 Notice of Proposed Rulemaking, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, rel. April 17, 2018 ("Notice").

2 Notice ¶ 1.

3 Zenji Nakazawa, Public Safety and Consumer Protection Advisor, Office of FCC Chairman Pai, Remarks at the International Institute of Communications, Telecommunications, and Media Forum (May 25, 2018), *available at* https://www.fcc.gov/document/zenji-nakazawa-remarks-public-safety-communications-technology.

historical direction, the FCC has rightfully taken an appropriate step forward with regard to an examination of these issues with this proceeding on federal funds distributed through the Universal Service Fund ("USF"). While the Commission's proposals in this matter are necessary, they should be considered only a beginning. As described in more detail below, the Commission can and should ensure that the scope of its efforts to respond to critical supply chain vulnerabilities addresses also those that may impact the most critical of the Nation's communications networks – those that serve the Nation's first responders.

With respect to the instant proposals, the Commission should adopt the necessary rules and policies to prevent USF funds from being used to purchase or obtain equipment or services produced or provided by companies that pose a risk to national security and the integrity of communications networks or the communications equipment supply chain. Congress and executive branch agencies have raised concerns that state actors, such as China and Russia, have engaged in cyberespionage in the United States and have taken action to address such concerns. For example, on December 20, 2017, a group of 18 Senators and Representatives expressed their recommendations in a letter to Chairman Pai that "the United States . . . view with suspicion the continued penetration of the U.S. telecommunications market by Chinese telecommunications companies," and that U.S. government systems and contractors "should not include Huawei or ZTE equipment."[4] This letter was sent only days after passage of the National Defense Authorization Act of 2018, which includes Section 1654that prohibits the Secretary of Defense from procuring, obtaining, extending or renewing a contract to procure or obtain, any equipment produced by Huawei Technologies Company or ZTE Corporation to carry out any nuclear

[4] Letter from Senator Tom Cotton *et al.*, U.S. Senate, to Hon. Ajit Pai, Chairman, FCC, Dec. 20, 2017, *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-349859A2.pdf.

deterrence mission of the Department of Defense.[5] NDAA 18 also took action to ban banning the Defense Department from using any and all products developed or provided by Kaspersky Lab.[6]

Most recently, the U.S. House of Representatives passed H.R. 5515, the National Defense Authorization Act for Fiscal Year 2019, which would, among other things, prohibit all Federal agencies from procuring or obtaining, renewing or extending a contract to obtain or procure, or entering into a contract with an entity that uses any equipment, system, or service with telecommunications equipment from Huawei or ZTE.[7]

The USF funds networks in every state, territory, and tribal region of the United States. Given the reach of these networks and the Nation's reliance on them, the Commission's proposal is consistent with its core mandate to protect the reliability and resiliency of these networks by guarding these networks from the introduction and use of equipment and services deemed to be a threat.

In order to identify companies that pose a national security threat to the integrity of communications networks or the communications supply chain, the Commission should publish a list of prohibited suppliers, identified by Congress as well as executive branch agencies with the appropriate security-based expertise to inform the list such as the Department of Homeland Security, the Department of Justice, the Department of Defense, and the Department of Commerce. However, the Commission is best positioned to be the appropriate agency for

---

5 National Defense Authorization Act for Fiscal Year 2018, Pub. L. 115-91, § 1654 (2017).

6 *Id.* at § 1634.

7 H.R. 5515 was passed by the House of Representatives on May 24, 2018. As of June 1, 2018, the final text of the bill is not yet available as reported out of the House.

publishing a comprehensive list and notifying the communications industry as well as other stakeholders such as local and state governments of suppliers that pose threats to network integrity and national security. In sourcing this information from a wide array of specialized knowledge, the Commission will foster a whole-of-government approach to vendor identification and evaluation, which may include designating a lead agency and/or creation of an interagency process. And, as described further below, the Commission should use this list to inform additional steps in which it could modify its rules and programs to further protect American citizens from national security risks.

Collaboration between agencies will be important to this process going forward in order to ensure uniformity across the federal government and prevent confusion among industry stakeholders. However, it is also important that in developing an interagency process, the Commission must identify which actions by other federal entities would trigger the inclusion of a covered company in the list. Furthermore, the Commission should devise specific criteria that would illustrate how and why companies are included in the list in order to ensure consistency and to prevent the criteria of inclusion from being unnecessarily overbroad.

The recently passed H.R. 5515 contemplates an interagency process. For example, the bill reflects an amendment offered by Rep. Cheney (R-WY) that would require the Director of National Intelligence to develop a report in coordination with the Director of the FBI, and the Secretaries of State, Homeland Security, and Defense, detailing the threats to national security posed by certain companies, with particular emphasis on any evidence of malicious software or hardware that would enable unauthorized network access or control.[8] This report would be

[8] *Id.*, at § 880(c)(1).

shared with U.S. allies, partners, and U.S. cleared defense contractors and telecommunications services providers in classified form where appropriate, and an unclassified equivalent where necessary.[9]

As indicated above, the Commission's intent to protect the communications networks and supply chain from national security threats by way of the administration of USF is an appropriate step forward, however a broader examination is necessary. To that end, the Commission should expand the scope of its examination to address how to protect the most critical of communications networks and services subject to its oversight from such threats – those comprising public safety communications.

Land mobile radio (LMR) systems provide emergency first responder organizations such as police, fire, and ambulance services with mission critical communications. With approximately 10,000 different public safety LMR networks operating in the U.S. at the local, state and federal level, the Commission cannot afford to delay to act in defense of those who serve and protect and save lives on a daily basis.

Likewise, the infrastructure and equipment that serve the developing Next Generation 9-1-1 and First Responder Network Authority (FirstNet) must be protected from companies that would threaten these valuable networks with compromised technology. FirstNet's nationwide broadband wireless network will enable an interoperable platform for first responders throughout the United States to manage crises and effectively communicate with each other.

---

[9] *Id.*

In order to protect these vital networks and services and to ensure that the provision of emergency response services are continuously available to the public during times of crisis, Motorola Solutions recommends that the Commission examine through further rulemaking proceedings ways to address the importation and marketing of technology intended for public safety use that is designed, supplied, or manufactured by companies that have been identified as national security threats to the integrity of U.S. communications networks.[10] The adoption of restrictions would not be unprecedented. In 2011, the Department of Commerce barred Huawei from participating in FirstNet, prohibiting the company from testing its equipment for the network.[11] Similarly, the 2012 Middle Class Tax Relief and Job Creation Act prohibited any entity or person "who has been, for reasons of national security, barred by any agency of the Federal Government from bidding on a contract, participating in an auction, or receiving a grant" from receiving FirstNet and state implementation funds or participating in a spectrum auction.[12]

The Commission endeavors to protect our nation's communications networks and its communications supply chain. Its proposal to prohibit the use of USF funds to purchase equipment or services from any companies identified as posing a national security risk is a significant step toward protecting the integrity of our networks. However, while the Commission's proposal can benefit some aspects of public safety communications, the

---

[10] For example, the Commission could consider possible modifications to its rules concerning the importation and marketing of RF devices in order to impose restrictions on the commercial activities of those companies on the list of suppliers that pose threats to network integrity and national security.

[11] Eli Lake, *U.S. Blocks China Telecom Bid to Build Wireless Network Over Spying Concerns*, THE DAILY BEAST (Oct. 11, 2011), at https://www.thedailybeast.com/us-blocks-china-telecom-bid-to-build-wireless-network-over-spying-concerns.

[12] Middle Class Tax Relief and Job Creation Act of 2012, Pub. L. No. 112-96, 126 STAT. 156 (2012).

Commission should take this opportunity to take a broader approach to address supply chain vulnerabilities affecting public safety communications that would not be necessarily covered by a rule that only encompasses the USF.

Respectfully Submitted,

/*S/ Frank Korinek*
Frank Korinek
Director of Government Affairs
Spectrum and Regulatory Policy
Motorola Solutions, Inc.
1455 Pennsylvania Avenue NW
Suite 900
Washington, DC 20004
(202) 371-6900

June 1, 2018